QSC18 | QUALYS SECURITY CONFERENCE 2018

Qualys Indication of Compromise

Bringing IOC to the Next Level

Chris Carlson
VP, Product Management, Qualys, Inc.

Vulnerabilities are Low Hanging Fruit

Early 2010s

Zero-day Vulnerabilities

Today

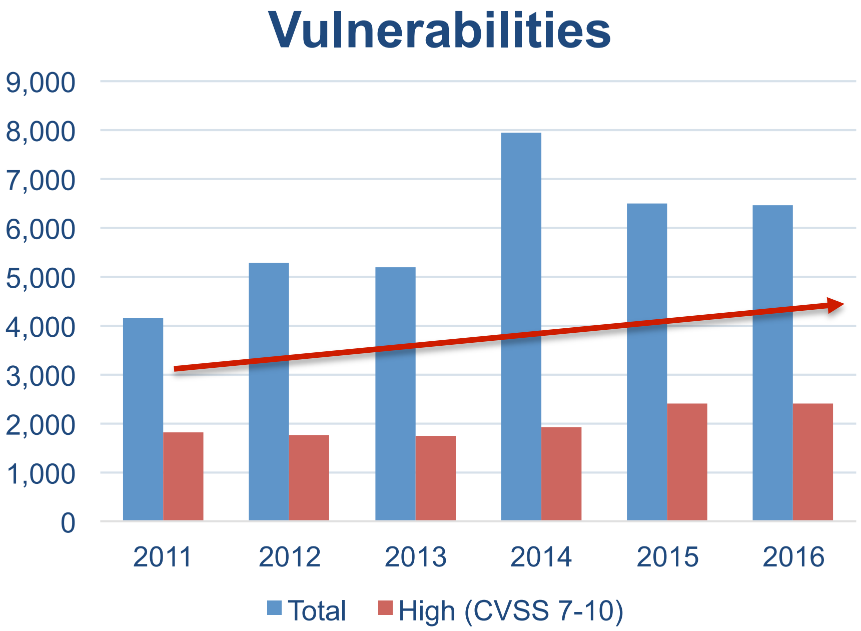
Rapidly weaponizing newly-disclosed vulnerabilities

Known Critical Vulnerabilities are Increasing

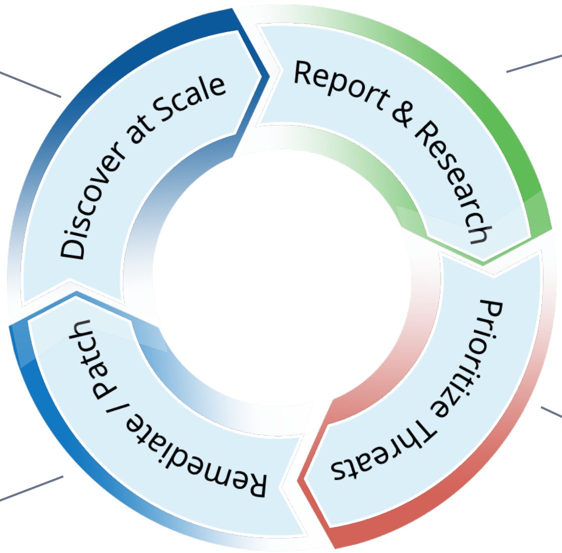
6-7K vulnerabilities are disclosed each year

30-40% are ranked as "High" or "Critical" severity

"**Mean Time to Weaponize**" is rapidly decreasing y/y



Vulnerability Management Lifecycle



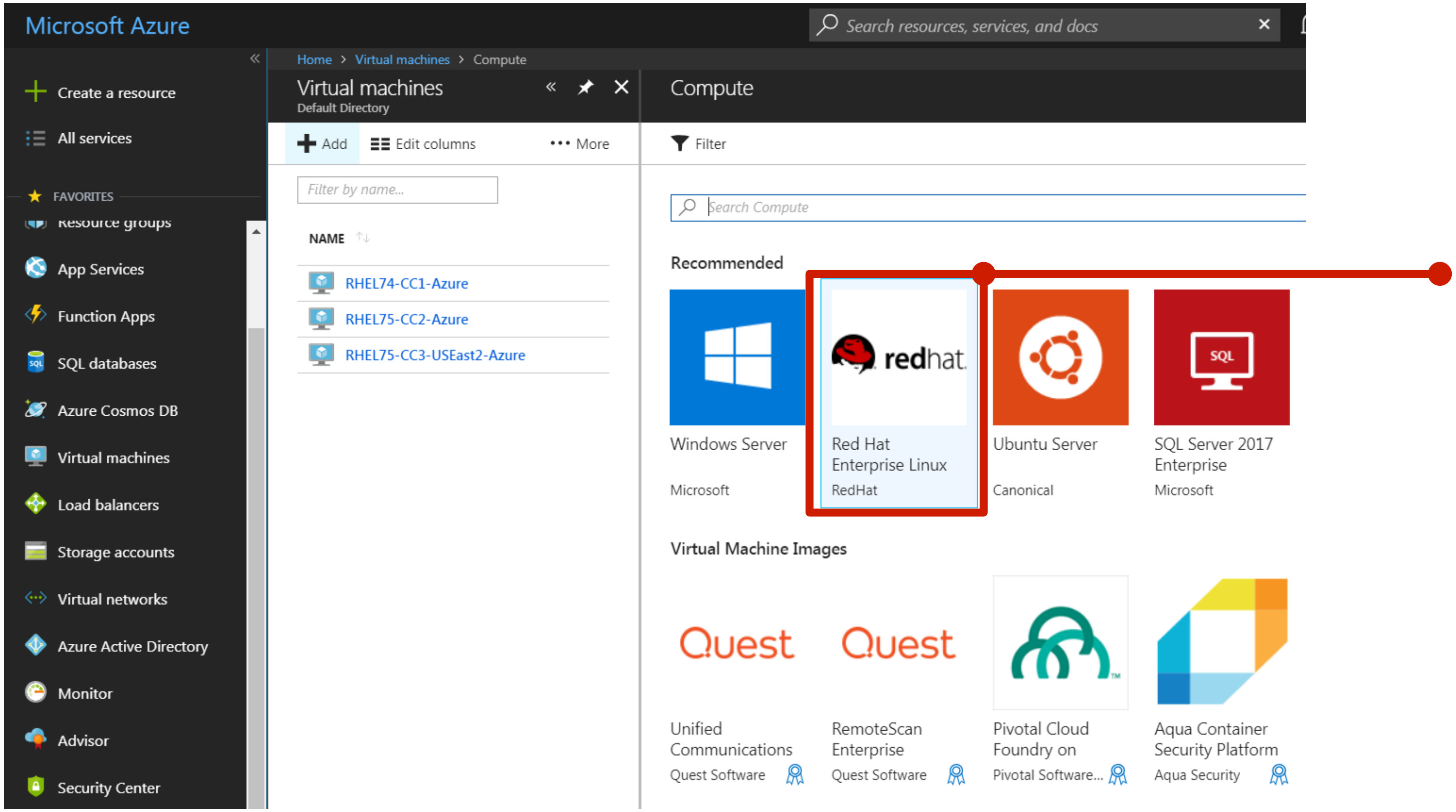
Asset Inventory

Vulnerability Management

Threat Risk and Prioritization

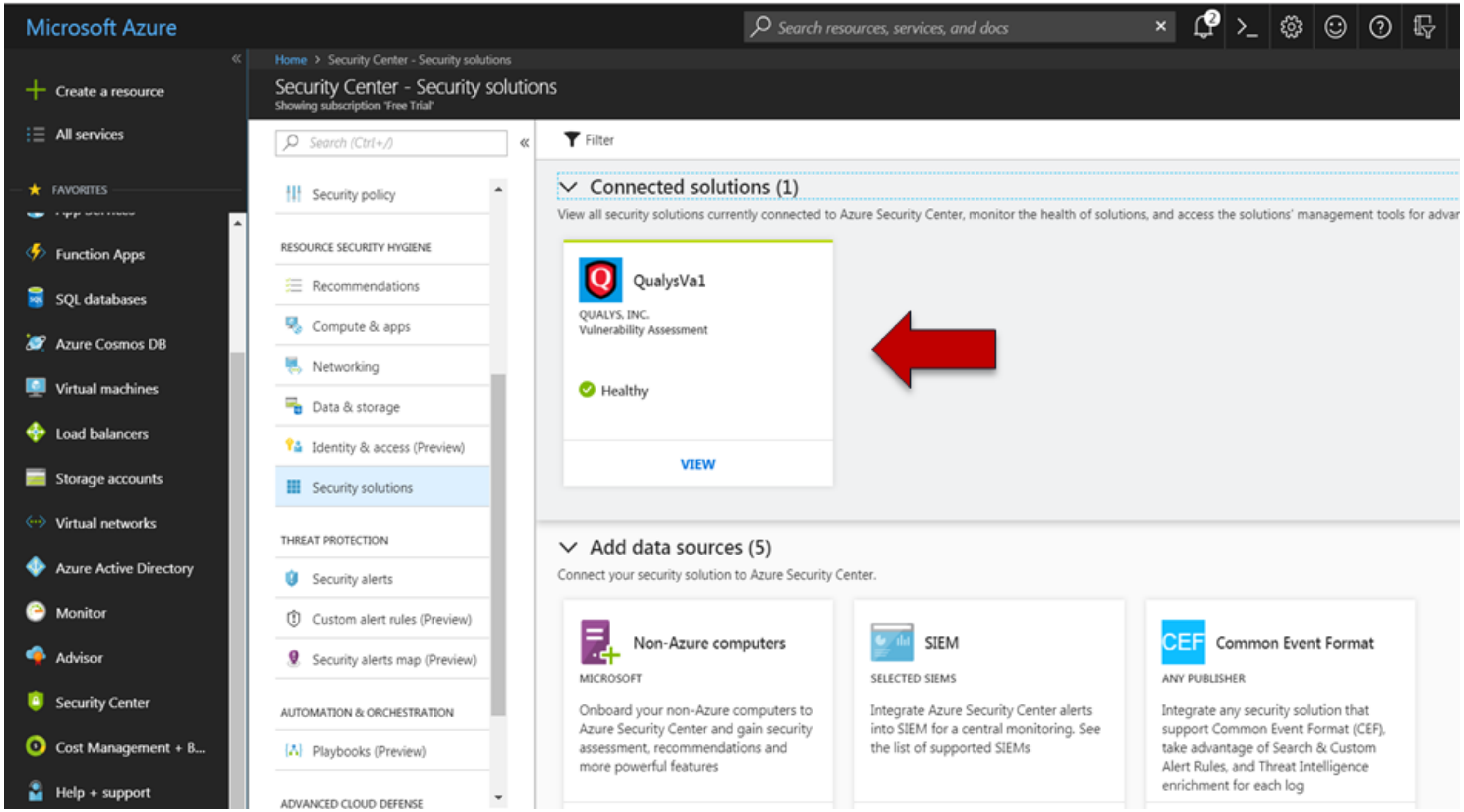
Patch Management

Vulnerability Spread at Speed of DevOps



Red Hat 7.4 Marketplace Image

Auto-Deploy Qualys Cloud Agent



View all security solutions currently connected to Azure Security Center, monitor the health of solutions, and access the solutions' management tools for advar

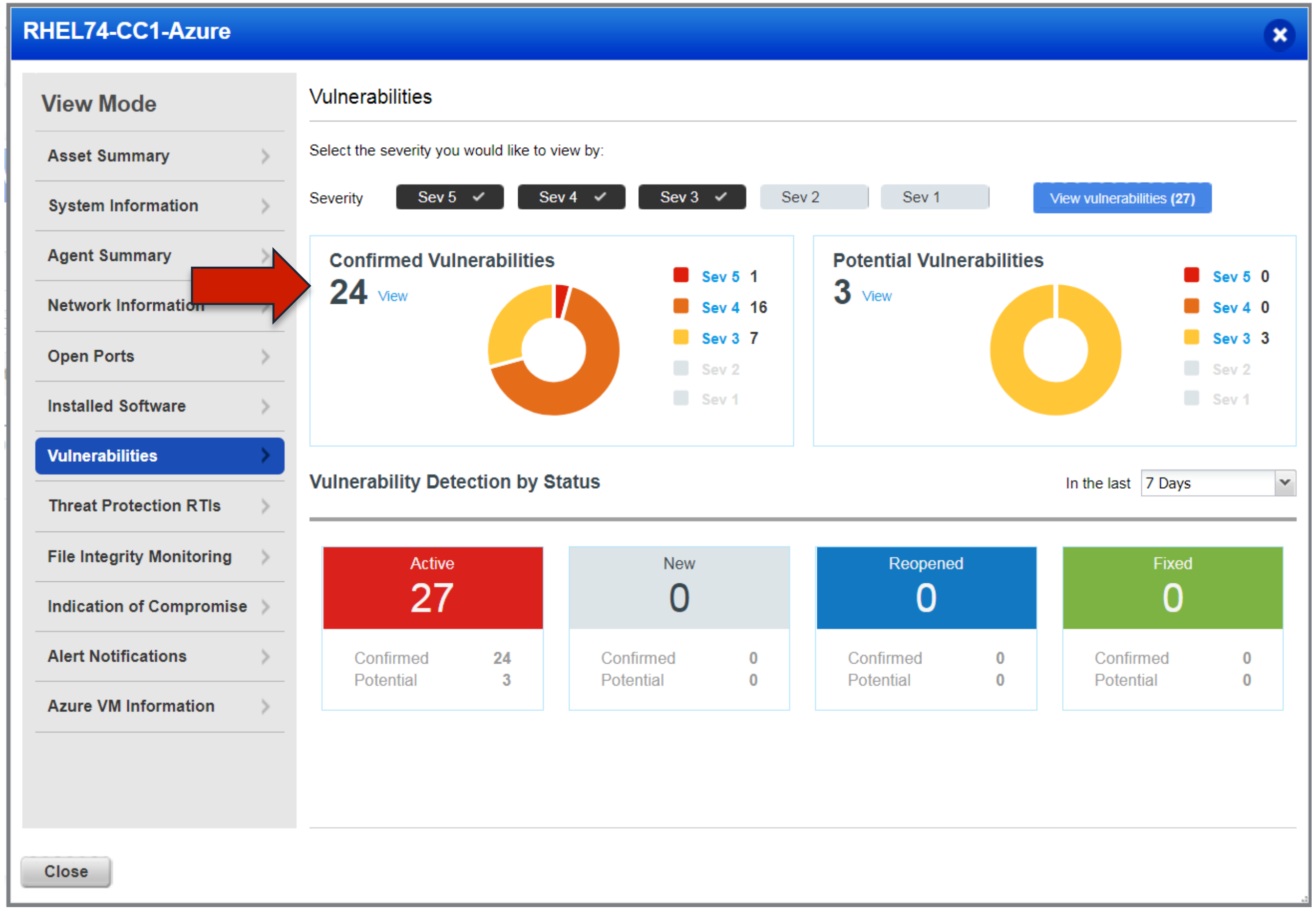
Connect your security solution to Azure Security Center.

Onboard your non-Azure computers to Azure Security Center and gain security assessment, recommendations and more powerful features

Integrate Azure Security Center alerts into SIEM for a central monitoring. See the list of supported SIEMs

Integrate any security solution that support Common Event Format (CEF), take advantage of Search & Custom Alert Rules, and Threat Intelligence enrichment for each log

Vulnerability Results



RHEL74-CC1-Azure

Vulnerabilities

Select the severity you would like to view by:

Severity: Sev 5 ✓ Sev 4 ✓ Sev 3 ✓ Sev 2 Sev 1 — View vulnerabilities (27)

Confirmed Vulnerabilities 24 View

🟥 Sev 5	1
🟧 Sev 4	16
🟨 Sev 3	7
Sev 2	
Sev 1	

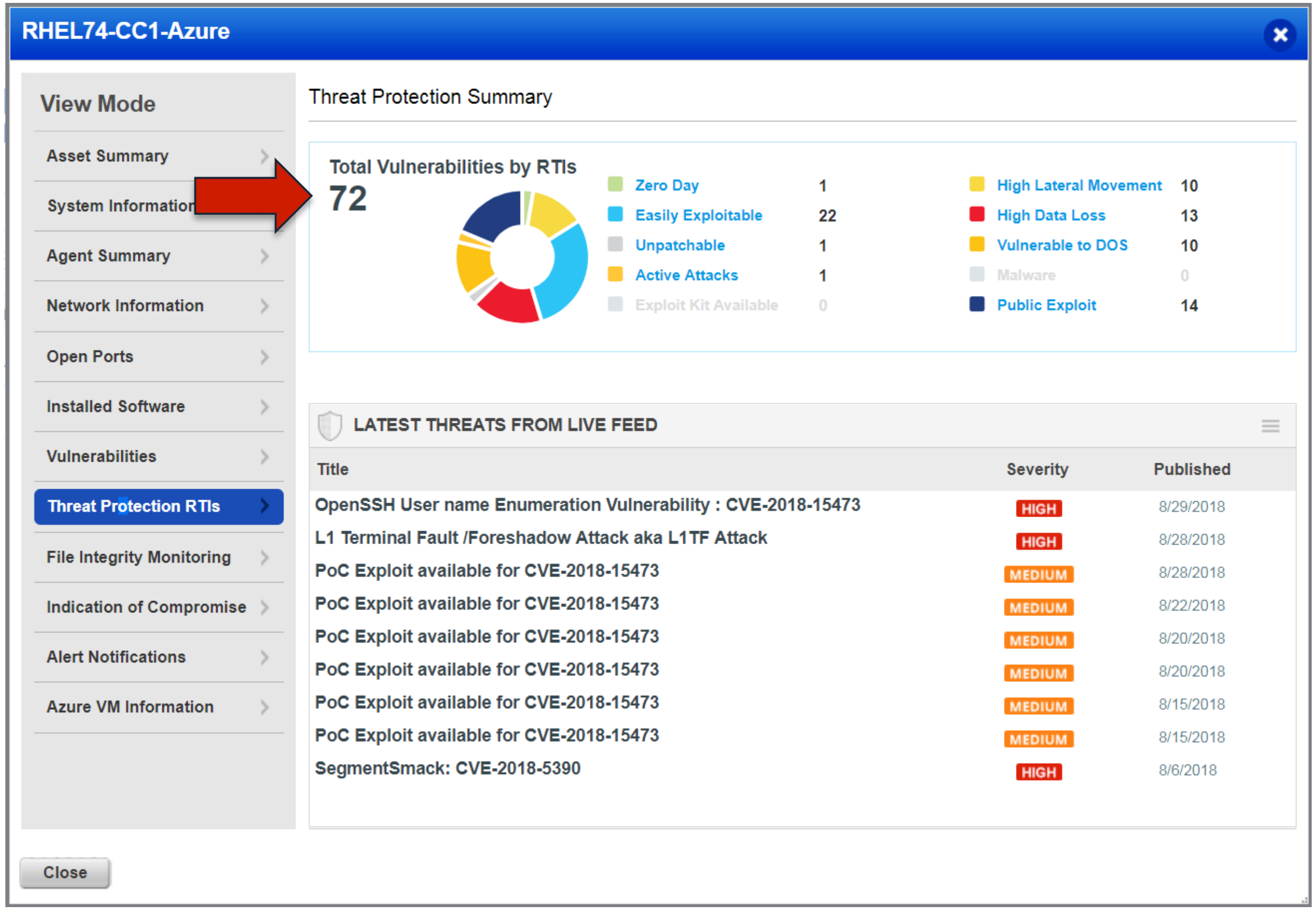
Potential Vulnerabilities 3 View

🟥 Sev 5	0
🟧 Sev 4	0
🟨 Sev 3	3
Sev 2	
Sev 1	

Vulnerability Detection by Status — In the last 7 Days

	Active	New	Reopened	Fixed
	27	0	0	0
Confirmed	24	0	0	0
Potential	3	0	0	0

Threat Protection: Exploitability Opportunity



Threat Protection Summary

Total Vulnerabilities by RTIs

72

🟩 Zero Day	1	🟨 High Lateral Movement	10
🟦 Easily Exploitable	22	🟥 High Data Loss	13
⬜ Unpatchable	1	🟨 Vulnerable to DOS	10
🟧 Active Attacks	1	⬜ Malware	0
⬜ Exploit Kit Available	0	🟦 Public Exploit	14

LATEST THREATS FROM LIVE FEED

Title	Severity	Published
OpenSSH User name Enumeration Vulnerability : CVE-2018-15473	HIGH	8/29/2018
L1 Terminal Fault /Foreshadow Attack aka L1TF Attack	HIGH	8/28/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/28/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/22/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/20/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/20/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/15/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/15/2018
SegmentSmack: CVE-2018-5390	HIGH	8/6/2018

Qualys.

Get Proactive – Reduce the Attack Surface

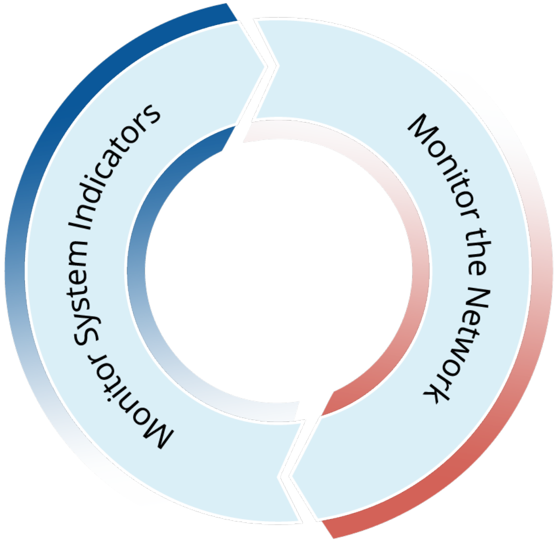
Immediately Identify Vulnerabilities in Production

Notify IT Asset Owner to Patch/Stop the Instance

Control Network Access / Cloud Security Groups

Add Detection and Response – Endpoint & Network

Proactively Hunt, Detect, and Respond



Indication of Compromise

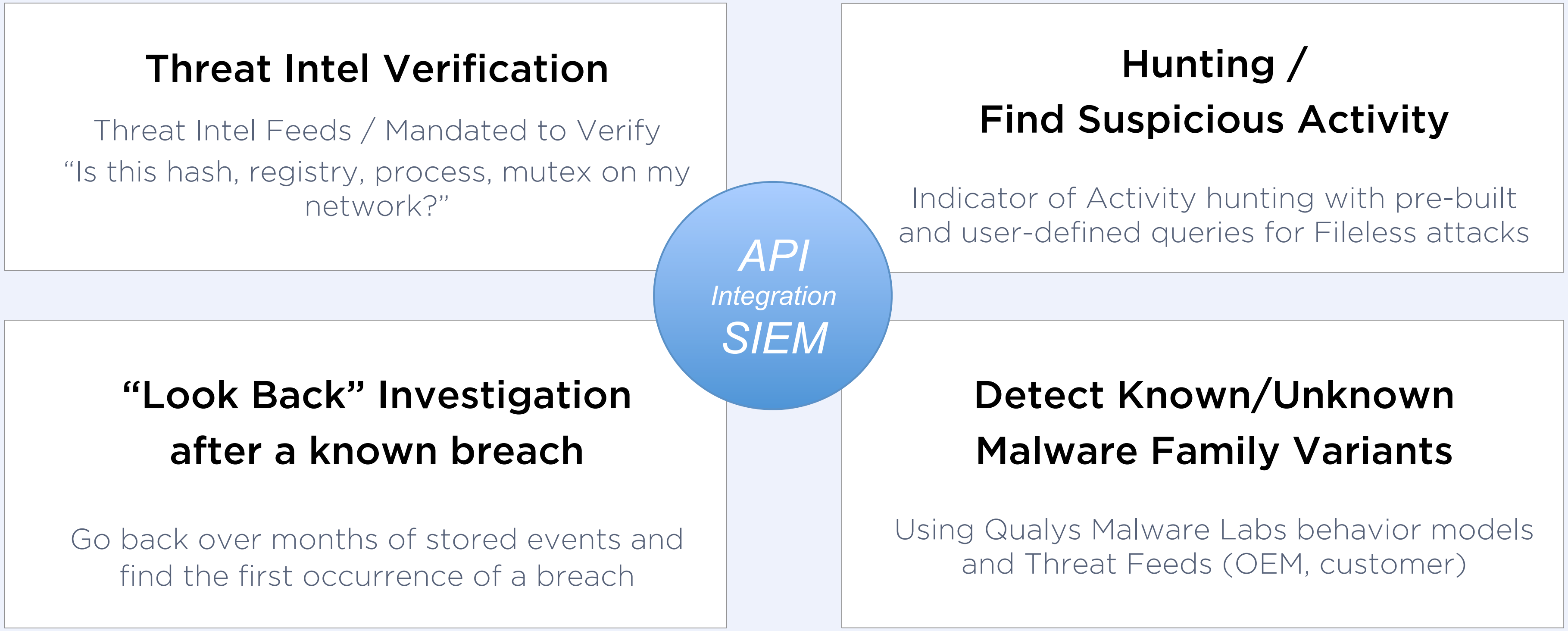
Detect IOCs, IOAs, and verify Threat Intel

Passive Network Sensor

What new devices are on the network? Are there new/ different traffic patterns?

Qualys IOC Use Cases –

Visibility Beyond AV



Threat Intel Verification

Threat Intel Feeds / Mandated to Verify
“Is this hash, registry, process, mutex on my network?”

Hunting / Find Suspicious Activity

Indicator of Activity hunting with pre-built and user-defined queries for Fileless attacks

API
Integration
SIEM

“Look Back” Investigation after a known breach

Go back over months of stored events and find the first occurrence of a breach

Detect Known/Unknown Malware Family Variants

Using Qualys Malware Labs behavior models and Threat Feeds (OEM, customer)

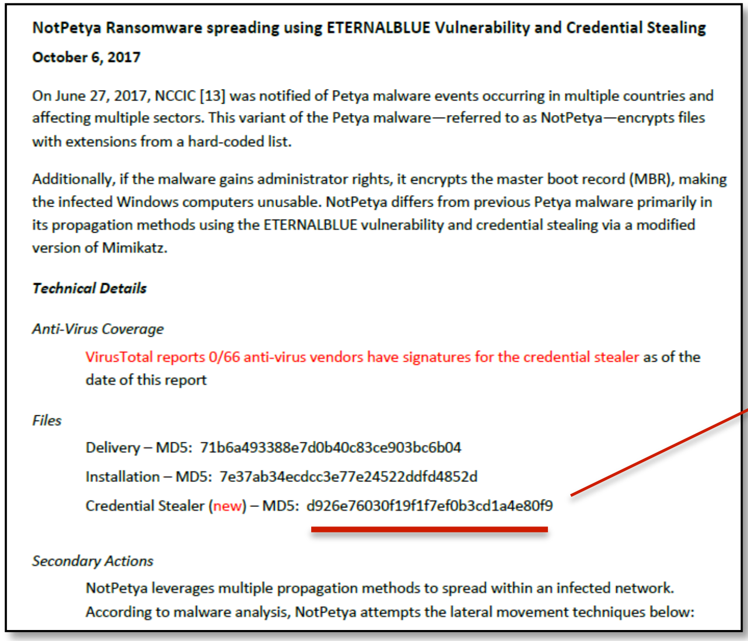
Organizations Struggle to Answer Basic Questions

Are these hashes on/running in my network?
Are these mutexes / processes / registry keys?

Did any endpoints connect to these IPs / Domains?
Are there any connections to TOR exit nodes?

What system is the first impacted? *“Patient Zero”*
Did this spread to others systems? When?

Threat Intel Verification



NotPetya Ransomware spreading using ETERNALBLUE Vulnerability and Credential Stealing

October 6, 2017

On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list.

Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods using the ETERNALBLUE vulnerability and credential stealing via a modified version of Mimikatz.

Technical Details

Anti-Virus Coverage

VirusTotal reports 0/66 anti-virus vendors have signatures for the credential stealer as of the date of this report

Files

Delivery – MD5: 71b6a493388e7d0b40c83ce903bc6b04

Installation – MD5: 7e37ab34ecdcc3e77e24522ddfd4852d

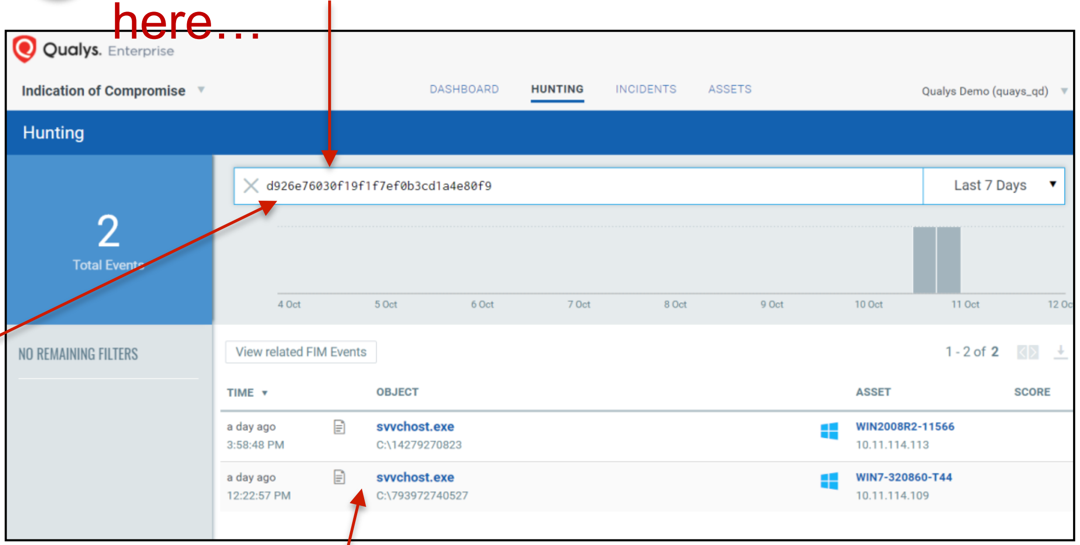
Credential Stealer (new) – MD5: d926e76030f19f1f7ef0b3cd1a4e80f9

Secondary Actions

NotPetya leverages multiple propagation methods to spread within an infected network. According to malware analysis, NotPetya attempts the lateral movement techniques below:

1 Threat Intelligence lists attack information …

2 Search for the file hash here…

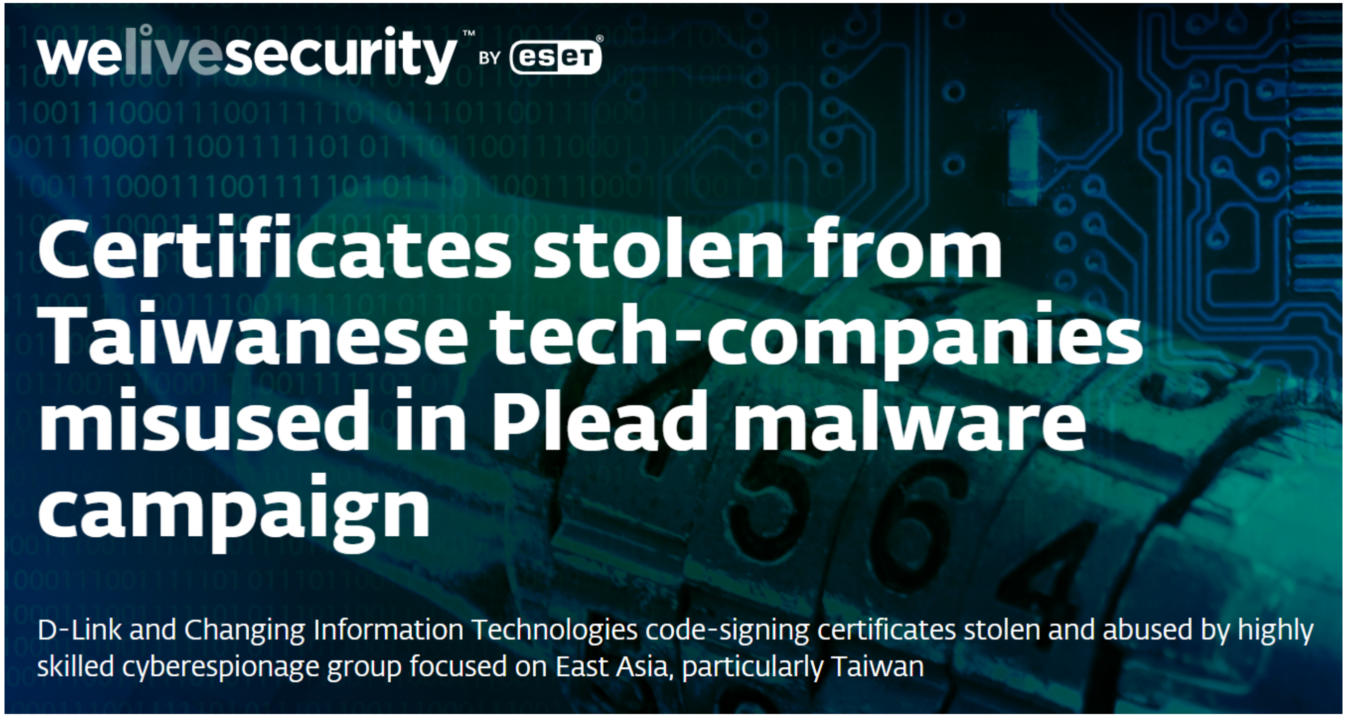


d926e76030f19f1f7ef0b3cd1a4e80f9 | Last 7 Days

TIME	OBJECT	ASSET	SCORE
a day ago 3:58:48 PM	svvchost.exe C:\14279270823	WIN2008R2-11566 10.11.114.113	
a day ago 12:22:57 PM	svvchost.exe C:\793972740527	WIN7-320860-T44 10.11.114.109	

3 Find the object there.

Malware Hides with Stolen Code-Signing Certificates



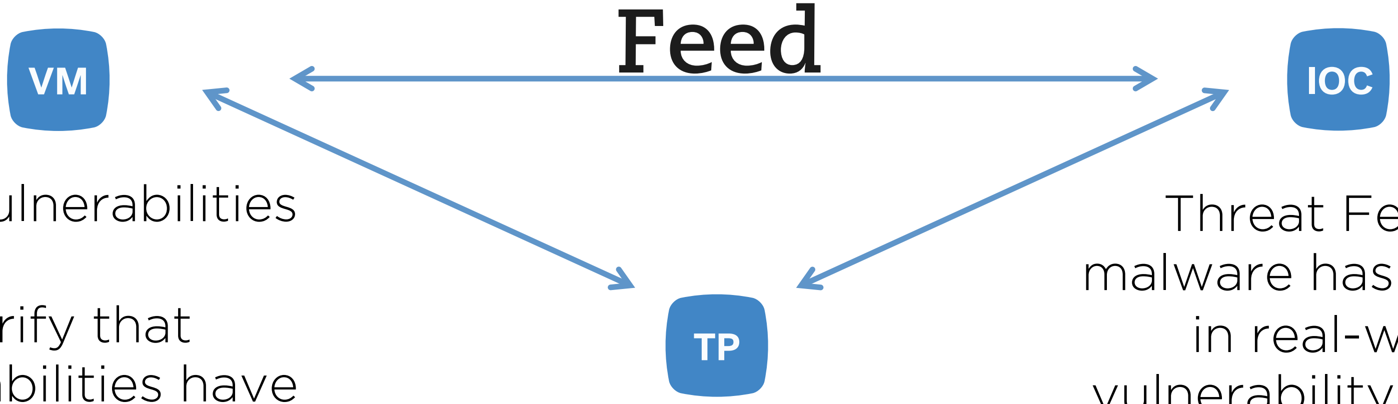
welivesecurity™ BY eset®

Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign

D-Link and Changing Information Technologies code-signing certificates stolen and abused by highly skilled cyberespionage group focused on East Asia, particularly Taiwan

https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/

New IOC CVE - File Reputation Threat Feed



Find Vulnerabilities

Verify that vulnerabilities have been remediated

Threat Feed of malware hashes used in real-world vulnerability exploits

Prioritize vulnerability remediation based on successful attacks in your network

Real-Time Indicators for which vulnerabilities have known / POC exploits

Prioritize vulnerability remediation on likelihood of attack

DEMO

IOC

Indication of Compromise

Threat Intel Verification
Hunting
Alerting
Create Emergency Patch Job from CVE Exploitation

18fc1b9b29a2d281ec9310f9f226ad77e3cb9c558f696c37390bbac72baa8ba8
168.63.129.16

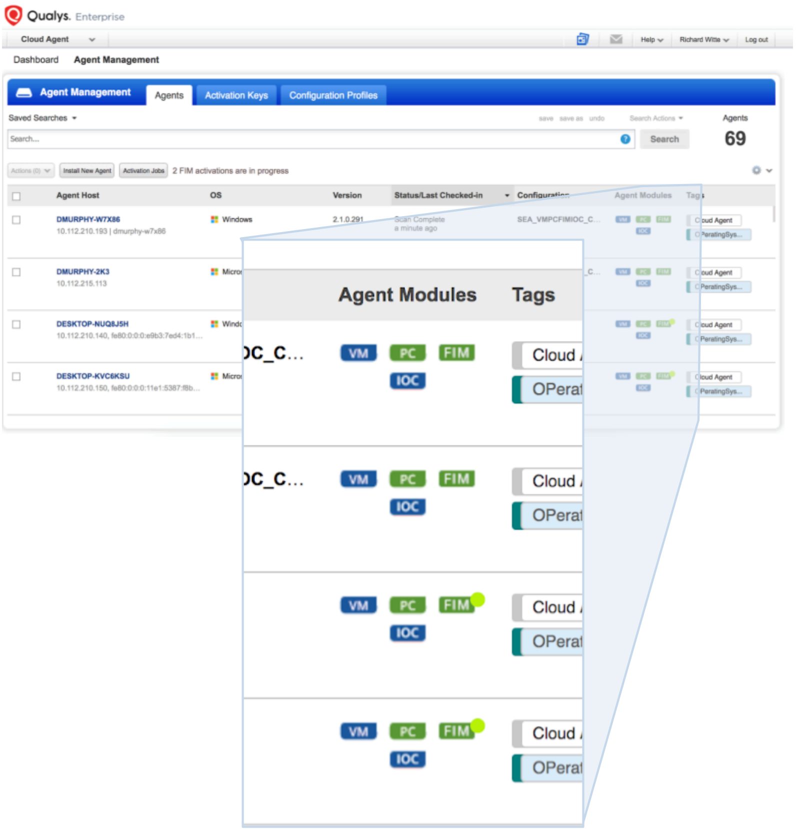
Qualys Cloud Agent

IT, Security, Compliance Apps

- AI Asset Inventory
- VM Vulnerability Management
- PC Policy Compliance
- IOC Indication of Compromise Detection
- FIM File Integrity Monitoring

Upcoming IT App (Beta November 2018)

- PM Patch Management



2 FIM activations are in progress

Agent Host	OS	Version	Status/Last Checked-in	Configuration	Agent Modules	Tags
DMURPHY-W7X86 10.112.210.193 | dmurphy-w7x86	Windows	2.1.0.291	Scan Complete a minute ago	SEA_VMPCFIMIOC_C...	VM PC FIM IOC	Cloud Agent OPeratingSys...
DMURPHY-2K3 10.112.215.113	Micro			C...	VM PC FIM IOC	Cloud Agent OPeratingSys...
DESKTOP-NUQ8J5H 10.112.210.140, fe80:0:0:0:e9b3:7ed4:1b1...	Windo				VM PC FIM IOC	Cloud Agent OPeratingSys...
DESKTOP-KVC6KSU 10.112.210.150, fe80:0:0:0:11e1:5387:f8b...	Micro				VM PC FIM IOC	Cloud Agent OPeratingSys...

QSC 18 | QUALYS SECURITY CONFERENCE 2018

Thank You

Chris Carlson
ccarlson@qualys.com